

Department of Veterans Affairs

§ 1.602

data, including service-connected medical conditions, income data, dependency data, deduction data, payment data, educational facility and program data (except chapter 32 benefits), and education program contribution and delimiting data (except chapter 32 benefits).

(2) Access to this information will currently be through the inquiry commands of BINQ (BIRLS (Beneficiaries Identification and Records Location Subsystem) Inquiry), SINC (Status Inquiry), MINQ (Master Record Inquiry), PINQ (Pending Issue Inquiry) and TINQ (Payment History Inquiry). The identifying information received from BIRLS to representative inquiries will be limited to file number, veteran's name, date of death, folder location and transfer date of folder, insurance number, insurance type, insurance lapse date and insurance folder jurisdiction.

(d) Sections 1.600 through 14.603 are not intended to, and do not:

(1) Waive the sovereign immunity of the United States; or

(2) Create, and may not be relied upon to create, any right or benefit, substantive or procedural, enforceable at law against the United States or the Department of Veterans Affairs.

[59 FR 47084, Sept. 14, 1994. Redesignated and amended at 73 FR 29870, 29879, May 22, 2008]

§ 1.601 Qualifications for access.

(a) An applicant for read-only access to VBA automated claims records from a location other than a VA Regional Office must be:

(1) An organization, representative, attorney or agent approved or accredited by VA under §§14.626 through 14.635; or

(2) An attorney of record for a claimant in proceedings before the Court of Veterans Appeals or subsequent proceedings who requests access to the claimant's automated claims records as part of the representation of the claimant.

(b) The hardware, modem and software utilized to obtain access, as well as their location, must be approved in advance by VBA.

(c) Each individual and organization approved for access must sign and return a notice provided by the Regional Office Director (or the Regional Office

Director's designee) of the Regional Office of jurisdiction for the claim. The notice will specify the applicable operational and security requirements for access and an acknowledgment that the breach of any of these requirements is grounds for disqualification from access.

[59 FR 47084, Sept. 14, 1994. Redesignated at 73 FR 29870, May 22, 2008]

§ 1.602 Utilization of access.

(a) Once an individual or organization has been issued the necessary passwords to obtain read-only access to the automated claims records of individuals represented, access will be exercised in accordance with the following requirements:

(1) The individual or organization will obtain access only from equipment and software approved in advance by the Regional Office from the location where the individual or organization primarily conducts its representation activities which also has been approved in advance;

(2) The individual will use only his or her assigned password to obtain access;

(3) The individual will not reveal his or her password to anyone else, or allow anyone else to use his or her password;

(4) The individual will access only the VBA automated claims records of VA claimants who are represented by the person obtaining access or by the organization employing the person obtaining access;

(5) The individual will access a claimant's automated claims record solely for the purpose of representing that claimant in a claim for benefits administered by VA;

(6) Upon receipt of the password, the individual will destroy the hard copy; no written or printed record containing the password will be retained; and

(7) The individual and organization will comply with all security requirements VBA deems necessary to ensure the integrity and confidentiality of the data and VBA's automated computer systems.

(b) An organization granted access shall ensure that all employees provided access in accordance with these

§ 1.603

38 CFR Ch. I (7–1–16 Edition)

regulations will receive regular, adequate training on proper security, including the items listed in §1.603(a). Where an individual such as an attorney or registered agent is granted access, he or she will regularly review the security requirements for the system as set forth in these regulations and in any additional materials provided by VBA.

(c) VBA may, at any time without notice:

(1) Inspect the computer hardware and software utilized to obtain access and their location;

(2) Review the security practices and training of any individual or organization granted access under these regulations; and

(3) Monitor an individual's or organization's access activities. By applying for, and exercising, the access privileges under §§1.600 through 1.603, the applicant expressly consents to VBA monitoring the access activities of the applicant at any time.

[59 FR 47084, Sept. 14, 1994. Redesignated and amended at 73 FR 29870, 29879, May 22, 2008]

§ 1.603 Disqualification.

(a) The Regional Office Director or the Regional Office Director's designee may revoke an individual's or an organization's access privileges to a particular claimant's records because the individual or organization no longer represents the claimant, and, therefore, the beneficiary's consent is no longer in effect. The individual or organization is no longer entitled to access as a matter of law under the Privacy Act, 5 U.S.C. 552a, and 38 U.S.C. 5701 and 7332. Under these circumstances, the individual or organization is not entitled to any hearing or to present any evidence in opposition to the revocation.

(b) The Regional Office Director or the Regional Office Director's designee may revoke an individual's or an organization's access privileges either to an individual claimant's records or to all claimants' records in the VBA automated claims benefits systems if the individual or organization:

(1) Violates any of the provisions of §§1.600 through 1.603;

(2) Accesses or attempts to access data for a purpose other than representation of an individual veteran;

(3) Accesses or attempts to access data other than the data specified in these regulations;

(4) Accesses or attempts to access data on a VA beneficiary who is not represented either by the individual who obtains access or by the organization employing the individual who obtains access;

(5) Utilizes unapproved computer hardware or software to obtain or attempt to obtain access to VBA computer systems;

(6) Modifies or attempts to modify data in the VBA computer systems.

(c) If VBA is considering revoking an individual's access under §1.603(b), and that individual works for an organization, the Regional Office of jurisdiction will notify the organization of the pendency of the action.

(d) After an individual's access privileges are revoked, if the conduct which resulted in revocation was such that it merits reporting to an appropriate governmental licensing organization such as a State bar, the VBA Regional Office of jurisdiction will immediately inform the licensing organization in writing of the fact that the individual's access privileges were revoked and the reasons why.

(e) The VBA Regional Office of jurisdiction may temporarily suspend access privileges prior to any determination on the merits of the proposed revocation where the Regional Office Director or the Director's designee determines that such immediate suspension is necessary in order to protect the integrity of the system or confidentiality of the data in the system from a reasonably foreseeable compromise. However, in such case, the Regional Office shall offer the individual or organization an opportunity to respond to the charges immediately after the temporary suspension.

[59 FR 47084, Sept. 14, 1994. Redesignated and amended at 73 FR 29870, 29879, May 22, 2008]

INVENTIONS BY EMPLOYEES OF DEPARTMENT OF VETERANS AFFAIRS

AUTHORITY: Sections 1.650 to 1.666 issued under sect. 1, 66 Stat. 811, 72 Stat. 1114; 35